様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ６ 月　 ８ 日現在

機関番号：１４３０１
研究種目：基盤研究(C)（一般）
研究期間：2017～2020
課題番号：１７Ｋ００１９９

研究課題名（和文）ID連携基盤における不正アクセス対策のための強固な認証セキュリティアーキテクチャ

研究課題名（英文）Strong Secure Authentication Architecture for Protection Against Unauthorized Access in ID Federation Platforms

研究代表者
中村　素典（Nakamura, Motonori）

京都大学・学術情報メディアセンター・教授

研究者番号：３０２６８１５６

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：インターネットにおける成りすましや不正アクセスによる犯罪等への対策として、オンライン認証の強化が課題である。本研究では、端末やサーバには脆弱性が存在していることを前提とし、一連の処理の途中で改ざんが行われることを防止するトランザクション認証と、複数の認証システムを併用した多信頼点認証方式を併用することで、一か所の脆弱性への攻撃だけでは不正アクセスを許してしまうことのない、安全性の高い次世代認証連携アーキテクチャを、シングルサインオン技術に基づくID連携フレームワーク上に構築する方法を提案し、その実現方法について検討を行った。

研究成果の学術的意義や社会的意義
不正アクセスの手口は年々巧妙化し、オンラインサービスに対する犯罪が増加している。その対策として認証強化が重要であるが、従来の手法はは一つのサーバに対する一度限りの認証処理となっているため、パスワード等の認証情報のフィッシングやウィルス感染によるスパイウエアの侵入による中間者攻撃に対して依然として脆弱であるという問題がある。本研究は、一連のオンライン処理の中で重要なタイミングで再認証を求めることにより継続的に認証を行う手法であるトランザクション認証と、一つのサーバのみを信頼しない多信頼点認証方式を組み合わせることで、こういった従来の不正アクセス手段を無力化し、安全なオンライン認証手段を実現する。

研究成果の概要（英文）：Spoofing and unauthorized access on the Internet are issues that need to be resolved to prevent crime, and strengthening online authentication is required as a countermeasure. In this research, we assume vulnerabilities of terminals and servers, and combine transaction authentication, which prevents tampering with a series of processes, and multi-factor authentication, which uses multiple authentication systems together. By using these methods together and applying them to the federated ID framework based on single sign-on technology, we propose a highly secure next-generation federated authentication architecture that does not allow unauthorized access and attacks only one vulnerability. We examined how to realize the system.

研究分野：コンピュータネットワーク

キーワード：ID連携　シングルサインオン　SAML　Shibboleth　多要素認証　セキュリティ

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

インターネット上に提供されるサービスにおいて、認証はネットワークの向こう側にいる利用者が、実際のサービス対象者であることを確認するために必要不可欠な手段である。近年、脆弱なパスワード認証が破られ被害を受ける事例が急増しており、利便性を保ちつつ認証を強固にしていくことは、安全な社会基盤を維持する上で社会共通の急務の課題である。

電子証明書やワンタイムパスワード等の高度な認証要素技術を組み合わせた多要素認証は、安全性向上に向けた取り組みの代表例であり、脆弱なパスワード認証の代替として実サービスへの導入も徐々に進んでいる。しかしながら、近年の不正アクセス事例には、ウィルス等のマルウェアに感染した PC が Web ブラウザに対して介入する MITB（Man in the Browser）によるものが登場しており、利用者の PC は健全であるとの仮定に基づく従来の認証技術では不正アクセス対策は十分ではない。そこで、認証における計算に処理内容を含める、いわゆるトランザクション認証と呼ばれる仕組みの採用が始まっている。ただし、トランザクション認証は、各サービスに特化された形で導入されることが一般的であり、汎用的な認証サービスにはなっていない。

一方、認証の汎用化に向けた取り組みとして、多数のサービスを利用する際の本人認証を統一しようとする動きがある。サービス毎に異なる ID とパスワードを使い分ける煩雑さを解消し管理コストを削減するために、シングルサインオン（SSO）の仕組みを活用して、あるサービスでの ID とパスワード等を他のサービスに対する認証にも利用できるように連携する取り組みが本格的に広がり始めている。このような連携は ID 連携（ID フェデレーション）と呼ばれ、多くは SAML（Security Assertion Markup Language）や OpenID 等の SSO 技術に基づいている。

ID 連携の認証基盤は、ユーザとの認証処理を担当する IdP（ID Provider）と、オンラインサービスを提供する SP（Service Provider）の 2 種類のサーバから構成される。認証処理は各オンラインサービス提供サーバから切り離され特定の IdP に集約されることから、パスワードの流通範囲が限定され、漏洩の可能性が低減する点がメリットである。しかし、現時点の ID フェデレーションでは、トランザクション認証への対応が考慮されていない。また、IdP 自体が脆弱であると、万一認証が破られた場合に同時に多くのオンラインサービスにも影響を及ぼす、いわゆる単一障害点となり得る。

２．研究の目的

背景で述べた二つの問題点、すなわち、認証後の一連の処理の途中での不正アクセスの介入の余地と、単一障害点となりうる認証サーバ（IdP）の脆弱性について、包括的に解決する汎用的な仕組みを実現し、今後の次世代 ID 連携基盤として利用できるようなセキュリティ技術の開発を目指す。

３．研究の方法

(1) トランザクション認証の汎用化

マルウェアに感染した PC において MITB（Man in the Browser）攻撃が想定される場合、従来の認証方式のままでは、認証が成功した後のセッションに介入され、オンラインバンキングサイトでの不正送金等の不正アクセスを防ぐことができない。このような不正アクセスを防ぐ一つの方法として、トランザクション認証方式がある。これは、重要な処理を行う際に、処理の内容も含めたワンタイムパスワードの計算を行い、処理の内容が改ざんされていないことを確認することで、介入を防止する方法である。このような対策は、複数のサービスが、認証サーバを共用する ID 連携においても有用であると考えられる。しかし、ID 連携基盤では、認証を行うサーバである IdP と、実際のサービスを提供する SP の 2 種類に役割が明確に分離されており、既存の実装では、IdP 側で行われる認証処理は、SP 側で行おうとする処理の内容を反映するようにはなっていない。そこで、ID 連携基盤の代表的な方式である SAML/Shibboleth および OpenID Connect に対して、トランザクション認証を実現するための方法を検討する。トランザクション認証の方式としては、OCRA（OATH Challenge-Response Algorithm）などがあり、これらの ID 連携基盤への親和性を検証する。特に、SP 側では様々な処理が行われる可能性があり、IdP 側での認証処理においては、あらゆる SP でのトランザクションに対応する必要があることから、汎用かつ安全性の高いユーザインタフェースについて検討を行う。

(2) 多信頼点認証方式

パスワードによる認証の脆弱性回避のために、電子証明書等を用いた認証や、複数の認証技術を組み合わせた多要素認証、さらに複数の通信路を併用することによる多経路認証といった、よ

り強力な認証方式への移行が始まりつつある。これらの技術の採用により、不正アクセスの可能性が低減されることが期待される。しかし、いずれの手法も、基本的に一つの認証サーバに信頼を置くモデルとなっている。一つの認証サーバの信頼性がますます重要となる ID 連携の展開を安全に推進するためには、万一、認証サーバに存在する脆弱性から侵入が発生しても、多くのサービスが被害を受けることのないようなアーキテクチャになっていることが望ましいが、現在の多くの認証プロトコルは、一つの認証サーバのみに依存するものがほとんどである。そこで、認証の信頼点を複数に分散させ、一つの認証サーバが侵入等の被害を受けても、他のサービスに被害が広がらない仕組みについて検討を行う。それらを多信頼点認証方式に対応させる方法について検討を行う。

４．研究成果

SAML を用いた ID 連携技術においては Shibboleth と呼ばれるオープンソースミドルウェアが広く利用されていることから、Shibboleth IdP の利用において、これまで広く利用されてきた ID/パスワードのような脆弱なものの代替となる、より認証強度の高い多要素認証方式の活用方法について調査を行った。Shibboleth IdP は 2016 年にバージョン 2 からバージョン 3 への移行が進められ、実装が大幅に変更されていることから、Shibboleth IdP バージョン 3 における多要素認証方式の利用方法について調査を行い、国立情報学研究所が運営する学術認証フェデレーション「学認」のウェブサイトにおいて、サポート情報として設定方法について公開した。
https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=26186832
利用者に求められる認証強度は、利用するサービス（SP: Service Provider）の内容ごとに異なることから、複数レベルの認証強度を設定して、それぞれの認証強度レベルごとに要求すべき最低限の認証手段（パスワード、証明書、認証トークン等）が設定できるようにし、SP 側から必要とする認証レベルが指定できる方法について調査を行った。アクセス元の IP アドレス等に基づくリスクベース認証にも対応する方法についても併せて提供している。
さらに、Shibboleth IdP バージョン 3 において、認証を強化するための MultiFactor 認証フローを利用した多要素認証の実現方法について情報をまとめ、Web サイトで提供を行うとともに、多要素認証のためのデバイスとして利用可能な Tiqr についても、Shibboleth IdP バージョン 3 対応を行った環境を構築し提供を行った。
https://meatwiki.nii.ac.jp/confluence/display/tiqr/Home

認証の対象とする処理内容を利用者およびシステム側で共に確認し、途中での処理内容の改竄を防ぐトランザクション認証に関する調査としては、近年、認証プロトコル標準規格として検討が進められている FIDO の UAF においてトランザクション認証がサポートされていることから、その詳細について調査を行ったが、新たに定められた後継仕様である FIDO2 についても調査を進めた。また、本研究と並行して、京都大学において認証システムの強化の一環として多要素認証の導入を進めることとなり、その中でもオンライン認証の安全性や利便性に関する問題と対策について検討するとともに、提案システムの導入可能性について検討を行った。多要素認証の仕組みとして、Time-based One-Time Password とともに FIDO2 がサポートされることから、実環境における FIDO2 の使い勝手についても調査を行い知見を得た。
昨今の研究データ管理に関する環境整備が進む中、組織を越えた認証、すなわち ID 連携への需要がさらに高まってきている。異なる組織に属する研究者による共同研究を支援したり、研究者が組織を移っても研究が継続できるような研究用情報環境が求められるようになっきており、そのような研究者の活動も踏まえた認証基盤の検討がますます重要になってきている。このような動きは、本研究の延長線上にあるものであり、国立情報学研究所において、本研究の考え方をベースとし複数の認証システムと連携する「認証プロキシ」の開発を開始するとともに、次世代認証連携検討作業部会の設置をうけて連携ポリシーや属性情報の扱い方についてのより深い検討を始めている。

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計1件（うち招待講演　1件／うち国際学会　0件）

１．発表者名 西村 健
２．発表標題 Shibbolethの多要素認証対応と学認
３．学会等名 第12回統合認証シンポジウム（招待講演）
４．発表年 2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

セキュリティレベルを設定したSPに対する認証 https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=21438629 MultiFactor認証フロー(MFA)を用いた認証設定 https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=26186832 ユーザによる認証方式が選択できる設定 https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=21438798 TOTPを用いた多要素認証方式の導入 https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=29233817 Shibbolized Tiqr https://meatwiki.nii.ac.jp/confluence/display/tiqr/Home MultiFactor認証フロー(MFA)を用いた認証設定 https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=26186832 MultiFactor認証フローを用いた認証設定 https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=26186832

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	西村　健 (Nishimura Takeshi) (50334272)	国立情報学研究所・学術基盤課・特任研究員 (62615)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関